Patent claims

1. A method for checking the authenticity of a first communication subscriber in a communications network,
   - in which a first fault information item is formed in the first communication subscriber using a fault detection data item of the service provider and an information item relating to a random data item;
   - in which a second fault information item is formed in a second communication subscriber in the communications network using a fault detection data item of the second communication subscriber and the information item relating to the random data item;
   - in which the authenticity of the first communication subscriber is checked using the first fault information item and the second fault information item.

2. The method as claimed in claim 1, in which a difference is determined between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

3. The method as claimed in claim 2, in which the difference is limited.

4. The method as claimed in one of claims 1 to 3, used within the scope of a mobile phone system.

5. An arrangement for checking the authenticity of a first communication subscriber in a communications network,

10009575.031802

- in which the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item;

10050356 - 030400

- in which a second communication subscriber is set up in the communications network in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item;
- in which the authenticity of the first communication subscriber can be checked using the first fault information and the second fault information.

6. The arrangement as claimed in claim 5, in which the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

7. The arrangement as claimed in claim 5 or 6, in which a fault detection data item is a sequential number.

8. The arrangement as claimed in one of claims 5 to 7, in which the information relating to the random data item is a random number.

9. The arrangement as claimed in one of claims 5 to 8, in which the first communication subscriber is a service provider in the communications network and/or the second communication subscriber is a service user in the communications network.

10. The arrangement as claimed in claim 9, in which the service provider is a mobile phone operator and/or the service user is a mobile phone.

11. The arrangement as claimed in one of claims 5 to 10, used within the scope of a mobile phone system.

10095765.031802

Abstract

Method and arrangement for checking the authenticity of a first communication subscriber in a communications network

In the method and the arrangement for checking the authenticity of a first communication subscriber in a communications network, a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In a second communication subscriber in the communications network, a second fault information item is formed using a fault detection data item of the second communication subscriber and the information relating to the random data item. The authenticity of the first communication subscriber is checked using the first fault information and the second fault information.

EP0993135A2

Patent claims

1. A method for checking the authenticity of a first communication subscriber in a communications network,
   - in which a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item which has been transmitted to the first communication subscriber by a second communication subscriber in the communications network;
   - in which the first fault information is transmitted to the second communication subscriber by the first communication subscriber,
   - in which a second fault information item is formed in the second communication subscriber using a fault detection data item of the second communication subscriber and the information item relating to the random data item;
   - in which the authenticity of the first communication subscriber is checked in the second communication subscriber using the first fault information item and the second fault information item.

2. The method as claimed in claim 1, in which a difference is determined between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

3. The method as claimed in claim 2, in which the difference is limited.

BEST AVAILABLE COPY

4. The method as claimed in one of claims 1 to 3, used within the scope of a mobile phone system.

5. An arrangement for checking the authenticity of a first communication subscriber in a communications network,

EP00957580

- in which the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item which has been transmitted to the first communication subscriber by a second communication subscriber in the communications network, and the first fault information item can be transmitted to the second communication subscriber;
- in which the second communication subscriber is set up in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item, and the authenticity of the first communication subscriber can be checked using the first fault information and the second fault information.

6. The arrangement as claimed in claim 5, in which the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

7. The arrangement as claimed in claim 5 or 6, in which a fault detection data item is a sequential number.

8. The arrangement as claimed in one of claims 5 to 7, in which the information relating to the random data item is a random number.

9. The arrangement as claimed in one of claims 5 to 8, in which the first communication subscriber is a service provider in the communications network and/or the second communication subscriber is a service user in the communications network.

ERSATZBLATT (REGEL 26)

10. The arrangement as claimed in claim 9, in which the service provider is a mobile phone operator and/or the service user is a mobile phone.

11. The arrangement as claimed in one of claims 5 to 10, used within the scope of a mobile phone system.

Description

Method and arrangement for checking the authenticity of a first communication subscriber in a communications network

The invention relates to a method and an arrangement for checking the authenticity of a first communication subscriber in a communications network.

In a communications network, data is generally transmitted between communication subscribers, for example a service provider and a service user. In order to protect a communications network against penetration of an unauthorized communication subscriber into the communications network, the authenticity of each communication subscriber is generally checked.

Document [1] discloses a method and an arrangement for checking the authenticity of a communication subscriber, in particular of a service provider or of a service user in a communications network.

The method known from document [1] and the corresponding arrangement are based on what is referred to as 3G TS 33.102 Version 3.0.0 Draft Standard, which describes a security architecture of a mobile phone system.

In Fig. 4, the procedure during the checking of the authenticity of a communication subcriber, such as is known from the document [1] is illustrated symbolically and parts thereof will be explained below briefly.

A transmission of data is illustrated in Fig. 4 by an arrow in each case. A direction of an arrow characterizes a transmission direction during a data transmission.

Fig. 4 shows a mobile phone system 400, comprising a user 401 of a communication service, for example a mobile phone, and a provider 402 of a communication service. The provider 402 comprises a dial-in network 403 with a dial-in network operator from which the user 401 locally requests a communication service, and a home

network 404 with a home network operator with which the user 401 is signed on and registered.

In addition, the user 401, the dial-in network 403 and the home network 404 each have a central processing unit with a memory, for example a server (central computing unit), with which processing unit the procedure described below is monitored and controlled and on which memory data is stored.

The dial-in network 403 and the home network 404 are connected to one another via a data line over which digital data can be transmitted. The user 401 and the dial-in network 403 are connected to one another via any desired transmission medium for the transmission of digital data.

During a communication, the user 401 dials 410 into the dial-in network 403. At the start of the communication, checking of both the authenticity of the user 401 and the authenticity of the provider 402 is carried out.

To do this, the dial-in network 403 requests 411 what is referred to as authentication data from the home network 404, with which data the authenticity of the user 401 and of the provider 402 can be checked.

The authentication data which is obtained from the home network 404 comprises a random number and a sequential number of the provider 402. The sequential number of

10005475.031802

the provider 402 is obtained in such a way that a counter of the provider 402 increases the sequential number of the provider 402 by the value 1 at each attempt at communication between the user

10009575.031802

401 and the provider 402.

It is to be noted that the random number and the sequential number of the provider 402 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is known from [1].

The home network 404 transmits 412 the requested authentication data to the dial-in network 403. The dial-in network 403 processes the received authentication data in a suitable way 413, and transmits 414 the processed authentication data to the user 401.

The user 401 checks 415 the authenticity of the provider 402 using a dedicated sequential number, which is handled in a way corresponding to the sequential number of the provider 402, and using the sequential number of the provider 402.

The procedure during the checking of the authenticity of the provider 402 is described in [1].

A result of the checking of the authenticity of provider 402, "authenticity of provider satisfactory" 416, "authenticity of provider satisfactory but sequential fault has occurred" 417 or "authenticity of provider not satisfactory" 418, is transmitted 419 from the user 401 to the provider 402.

In the case of the result "authenticity of provider satisfactory" 416, the dial-in network 403 checks 420 the authenticity of the user 401 as described in [1].

In the case of the result "authenticity of provider not satisfactory" 418, the communication is interrupted and/or restarted 421.

In the case of the result "authenticity of provider satisfactory but a sequential fault has occurred" 417, resynchronization takes place in such a way that the home network 404 transmits 422 a resynchronization request to the user 401. The user responds with a resynchronization response in which resynchronization data is transmitted 423 to the home network 404. The sequential number of the provider 402 is changed 424 as a function of the resynchronization response. The authenticity of the user 401 is then checked, as is known from [1].

The procedure described has the disadvantage that during checking of the authenticity of a communication subscriber, in particular during the checking of the authenticity of a service provider, a large amount of data has to be transmitted between the communication subscribers.

The invention is thus based on the problem of disclosing a method which is simplified and improved in comparison with the known method and the known arrangement, and a simplified and improved arrangement for checking the authenticity of a communication subscriber in a communications network.

The problem is solved by means of the methods and by means of the arrangements having the features in accordance with the independent patent claims.

In the method for checking the authenticity of a first communication subscriber in a communications network, a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In a second communication subscriber in the communications network, a second fault information item is formed

using a fault detection data item of the first communication subscriber and the information relating to the random data

10009575.031802

item.

The authenticity of the first communication subscriber is checked using the first fault information item and the second fault information item.

In the arrangement for checking the authenticity of a first communication subscriber in a communications network, the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In addition, the arrangement has a second communication subscriber in the communications network which is set up in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item. The authenticity of the first communication subscriber can be checked using the first fault information item and the second fault information item.

The checking of the authenticity of a communication subscriber in a communications network is to be understood as meaning method steps which are carried out in the wider sense with checking of the authorization of a communication subscriber for access to a communications network or participation in communication in a communications network.

This thus encompasses both method steps which are carried out within the scope of the checking of the authorization of a communication subscriber for access to a communications network and such method steps which are carried out within the scope of the processing or the administration of data which is used in the checking.

10095725.031802

Preferred developments of the invention are given in the dependent claims.

The developments described below relate to the method and to the arrangement.

The invention and the development described below can be implemented either using software or hardware, for example using a specific electrical circuit.

In one refinement, the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

A sequential number is preferably used as the fault detection data item.

In one refinement, the information relating to the random data item is a random number.

In one development, the checking of the authenticity is simplified by determining a difference between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

In one refinement, the checking of the authenticity is further improved with respect to the security of the communications network by limiting the difference.

One development is preferably used within the scope of a mobile phone system. In the mobile phone system, the service user is implemented as a mobile phone and/or the service provider is implemented as a mobile phone network operator.

An exemplary embodiment of the invention which is explained in more detail below is illustrated in the figures, in which figures:

Figure 1 shows a mobile phone system;

Figure 2 shows an outline in which checking of the authenticity of a communication subscriber is illustrated symbolically;

Figure 3 shows a flowchart in which individual method steps are illustrated during checking of the authenticity of a service provider in a communications network;

Figure 4 shows an outline in which checking of the authenticity of a communication subscriber in accordance with the 3G TS 33.102 Version 3.0.0 Standard is illustrated symbolically.

Exemplary embodiment: mobile phone system

A mobile phone system 100 is illustrated in <u>Fig. 1</u>. The mobile phone system 100 comprises a mobile phone 101, a local dial-in network 102 with a dial-in network operator 103 and a home network 104 with a home network operator 105.

The mobile phone 101 is signed on and registered in the home network 104.

In addition, the mobile phone 101, the dial-in network 102 and the home network 104 each have a central processing unit 106, 107, 108 with a memory 109, 110, 111, with which processing units 106, 107, 108 the procedure described below is monitored and controlled, and

on which memories 109, 110, 111 data is stored.

The dial-in network 102 and the home network 104 are connected to one another via a data line 112 via which digital data can be transmitted. The mobile phone 101 and the dial-in network 102 are connected to one another via any desired transmission medium 113 for transmitting digital data.

The procedure during the checking of the authenticity of the mobile phone 101 and the procedure during the checking of the authenticity of the home network 104 and/or of the home network operator 105 are illustrated symbolically in Fig. 2, and parts thereof will be explained below briefly.

The transmission of data in Fig. 2 is illustrated in each case by an arrow. A direction of an arrow characterizes a transmission direction during a data transmission.

The procedure which is described below and illustrated symbolically in Fig. 2 is based on what is referred to as a 3G TS 33.102 Version 3.0.0 Standard, which describes a security architecture of a mobile phone system and is described in [1].

During a communication, the mobile phone 201 dials 210 into the dial-in network 203. At the start of the communication, checking both of the authenticity of the mobile phone 201 and of the authenticity of the home network 204 and/or of the home network operator takes place.

To do this, the dial-in network 203 requests 211 authentication data from the home network 204, with which authentication data the authenticity of the user 201 and of the home network 204 and/or of the home network operator can be checked.

The authentication data which is determined by the home network 204 comprises a random number and a sequential number of the home network 204 (cf. Fig. 3 step 310). The sequential number of the home network 204 is determined in such a way that a counter of the home network 204 increases the sequential number of the home

network 204 by the value 1 at each attempt at communication between the mobile phone 201 and the home network 204.

It is to be noted that the random number and the sequential number of the home network 204 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is specified in [1].

The home network 204 transmits 212 the requested authentication data to the dial-in network 203. The dial-in network 203 processes the received authentication data in a suitable way 213 and transmits 214 the processed authentication data to the mobile phone 201.

The mobile phone 201 checks 215 the authenticity of the home network 204 using a dedicated sequential number which is handled in a way corresponding to the sequential number of the home network 204, and using the sequential number of the home network 204. In a way corresponding to the home network 204, the mobile phone 201 also has a counter.

The procedure during the checking of the authenticity of the home network 204 is described in [1]. Method steps which differ therefrom are described below.

What is referred to as overflow checking of the counter of the mobile phone 201 is carried out within the scope

of the checking of the authenticity of the home network 203. This overflow checking prevents overflowing of an acceptable numerical range of the counter of the mobile phone 201.

EP0969675A2

In the overflow checking, the following conditions are tested:

1) sequential number of the home network 204 > sequential number of the mobile phone 201;

2) sequential number of the home network 204 - sequential number of the mobile phone 201 < - predefinable deviation (1,000,000);

the following applying for the predefined deviation:

- predefinable deviation is sufficiently large in order to ensure, during normal or fault-free communications operation:

that the sequential number of the home network 204 - sequential number of the mobile phone 201 is not > predefinable deviation;

- the maximum permissable sequential number of the mobile phone 201/predefinable deviation is sufficiently large in order to ensure that the maximum permissible sequential number of the mobile phone 201 is not reached during operation.

The result of the checking of the authenticity of the home network 204, "authenticity satisfactory" 216, "authenticity satisfactory but a sequential fault has occurred" 217 or "authenticity not satisfactory" 218 is transmitted 419 to the home network 204 from the mobile phone 201.

In the case of the result "authenticity satisfactory" 216, the dial-in network 203 checks 220 the authenticity of the mobile phone 201, as described in [1].

EP0859519A2

In the case of the result "authenticity not satisfactory" 218, the communication is interrupted or restarted 221.

EP0969675A2

In the case of the result "authenticity satisfactory but a sequential fault has occurred" 217, resynchronization 222 takes place. Resynchronization is to be understood as a change of the sequential number of the home network 204.

For this purpose, the mobile phone 201 transmits 222 resynchronization data to the dial-in network 203.

The resynchronization data comprises the same random number which was transmitted within the scope of the authentication data, and the sequential number of the mobile phone 201 (cf. Fig. 3 step 320).

The dial-in network 203 processes the resynchronization data in a suitable way and transmits the processed resynchronization data to the home network 204.

The home network checks the sequential number of the mobile phone 201 and the sequential number of the home network 204 using the processed resynchronization data, and if appropriate changes 223 the sequential number of the home network 204 (cf. Fig. 3 step 330).

The home network 204 subsequently transmits new authentication data, which if appropriate comprises the changed sequential number of the home network 204, to the dial-in network 203.

In order to illustrate the described procedure, important steps 300 of the procedure are illustrated in Fig. 3.

Fig. 3 shows a first step 310 within the scope of which the authentication data (first fault information) is determined.

10036974.031802

The resynchronization data (second fault information) is determined within the scope of a second step 320.

The sequential number of the mobile phone and the sequential number of the home network are checked within the scope of a third step 330, using the resynchronization data.

An alternative of the first exemplary embodiment is described below.

In the alternative exemplary embodiment, a method is implemented in which the home network is made more reliable with respect to a data loss in the event of a system crash.

For this purpose, the current sequential number of the home network is stored in the memory of the home network, in each case at a predefinable time interval. A sequential number of the home network which has been lost during a system crash of the home network is restored in such a way that a predefinable additional value is added to the value of the stored sequential number. The predefinable additional value is dimensioned in such a way that exceeding of the sum of the sequential number of the mobile phone and the predefinable deviation is not exceeded.

In the alternative exemplary embodiment, the predefinable additional value is determined in such a way that an average number of authentication attempts on one day by the home network, which number is determined during operation of the communications network, is multiplied by a factor with the value 10.

10035745.031802

The following publication is cited in this document:

[1] 3G TS 33.102 Version 3.0.0 Draft Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999.

EP 0 969 615 A2

ART 34 AMDT

Rec'd PCT/PTO 17 DEC 2001
10/009975

Patent claims

1. A method for checking the authenticity of a first communication subscriber in a communications network,
   - in which a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item which has been transmitted to the first communication subscriber by a second communication subscriber in the communications network;
   - in which the first fault information is transmitted to the second communication subscriber by the first communication subscriber,
   - in which a second fault information item is formed in the second communication subscriber using a fault detection data item of the second communication subscriber and the information item relating to the random data item;
   - in which the authenticity of the first communication subscriber is checked in the second communication subscriber using the first fault information item and the second fault information item.

2. The method as claimed in claim 1, in which a difference is determined between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

3. The method as claimed in claim 2, in which the difference is limited.

Replacement Sheet

ART 34 AMDT

4. The method as claimed in one of claims 1 to 3, used within the scope of a mobile phone system.

5. An arrangement for checking the authenticity of a first communication subscriber in a communications network,

BEST AVAILABLE COPY

ART 34 AMDT

- in which the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item which has been transmitted to the first communication subscriber by a second communication subscriber in the communications network, and the first fault information item can be transmitted to the second communication subscriber;
- in which the second communication subscriber is set up in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item, and the authenticity of the first communication subscriber can be checked using the first fault information and the second fault information.

6. The arrangement as claimed in claim 5, in which the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

7. The arrangement as claimed in claim 5 or 6, in which a fault detection data item is a sequential number.

8. The arrangement as claimed in one of claims 5 to 7, in which the information relating to the random data item is a random number.

AMENDED SHEET

ART 34 AMDT

9. The arrangement as claimed in one of claims 5 to 8, in which the first communication subscriber is a service provider in the communications network and/or the second communication subscriber is a service user in the communications network.

ART 34 AMDT

10. The arrangement as claimed in claim 9, in which the service provider is a mobile phone operator and/or the service user is a mobile phone.

11. The arrangement as claimed in one of claims 5 to 10, used within the scope of a mobile phone system.

10059656 - 030800